**Instituto Tecnológico de Cancún**


**Materia:**

**Fundamentos de Telecomunicaciones**

**Tarea:**

**Investigar sobre**

**IDS Y IPS**

**Alumno:** **Aguilar Moreno Jorge Axel**

**Docente:** **Ismael Jiménez Sánchez**

**Horario:** **17:00 – 18:00**

**Ing.** **Sistemas Computacionales**

**5.-Semestre**

# IDS

## (Sistema de detención de instrucciones)

Es un programa utilizado para analizar la detección de supuestos intrusos en la red o un computador, basado en sensores virtuales, permiten monitorear el tráfico de la red, permitiendo así evitar posibles ataques.

El proceso de detección de intrusos, se lo define de la siguiente manera:

- Una base de datos con una recopilación de ataques anteriores.
- Un sistema actual debidamente configurado.
- Estado actual, referente en términos de comunicación y procesos.

### Tipos de IDS

1) **HIDS**. -**IDS** basados en **Host**, estos solo procesan determinadas actividades de los usuarios o computadoras.
2) **NIDS**. -**IDS** basados en **Red**, realizan sniffing en algún punto de la red, en busca de intrusos.
3) **DIDS**. -Es parte del **NIDS**, solo que, distribuido en varios lugares de la red, con un consolido en un solo banco de información.
4) **IDS** basados en **Log**, revisa los archivos de Logs en busca de posibles intrusos, se caracteriza por su precisión y completitud.

# IPS

## (Sistema de prevención de instrucciones)

Este sistema fue desarrollado en 1990, fue diseñado para monitorear el tráfico de una red, en tiempo real y prevenir que se filtre cualquier actividad maliciosa conocida como intrusión en la misma, cuando se produce la caída de un paquete o este pasa dañado o incompleto, en una transmisión de información, inmediatamente la red bloquea la transmisión por prevenir un posible ataque o deformaciones en la transferencia de datos, es considerado una mejora con respeto a los Firewalls, y Cortafuegos, su diseño es una evolución de los IDS (Sistema de Detección de Intrusos).

A diferencia de los IDS esta nueva tecnología no se limita solo a escuchar el trafico de la red y a mandar alertas en una consola, después de que ocurre una intrusión, el IPS funciona a nivel de la capa 7 tiene la capacidad de descifrar protocolos como HTTP, FTP y SMTP, algunos IPS permiten establecer reglas como se lo hace en los Firewalls.

### Tipos de IPS

- **IPS basados en host (HIPS)**: Esta aplicación de prevención de intrusiones reside en la dirección IP específica de un solo equipo, permite prevenir posibles ataques en los nodos débiles de una red es decir los host.
- **IPS basada en red (PIN):** Esta aplicación IPS es en hardware y cualquier acción tomada para prevenir una intrusión en una red específica de host (s) se hace de una máquina con otra dirección IP en la red (Esto podría ser en un front-end de cortafuegos).
- **IPS basado en red (PIN) vs IPS basado en host (HIPS)** HIPS puede manejar el tráfico cifrado y sin cifrar por igual, ya que puede analizar los datos después de que ha sido descifrado en el anfitrión.